National Weather Service

AUTOMATED SURFACE OBSERVING SYSTEM
System ID: NOAA8102

Operating Procedures For ASOS Password Management in Build 3.05

SOP Password_121510
Draft Date: 12/15/10

December 2010

Version 1.2

Document History			
Date	**Version #**	**Title**	**Approved by**
6/18/10	1.0	Initial Version for review	
8/12/10	1.1	Revised version for distribution	
12/13/10	1.2	Revised version for distribution	_____ Joseph Facundo W/OPS22

TABLE OF CONTENTS

Contents

List of Tables

1 INTRODUCTION

The Automated Surface Observing Systems (ASOS) program is a joint effort of the National Oceanic and Atmospheric Administration (NOAA) National Weather Service (NWS), the Federal Aviation Administration (FAA), and the Department of Defense (DOD). ASOS serves as the nation's primary surface weather observing network. ASOS supports weather forecast and warning activities and aviation operations and, at the same time, supports the needs of the meteorological, hydrological, and climatological research communities.

When it was deployed, in the mid-1990s, the ASOS network more than doubled the number of full-time surface weather observing locations. With the largest and most modern complement of weather sensors, ASOS significantly expanded the information available to forecasters and the aviation community.

NWS prepared the documentation to support the first Certification and Accreditation package for NWS ASOS to obtain an Authority to Operate (ATO) in May 2007. The Authorizing Official (AO) approved the subsequent ATO in March 2010. The AO is the Director, Office of Operational Systems (OOS).

Since 1992, when the first ASOS sites were commissioned, ASOS users have used group passwords. Group passwords do not meet the password policy and procedures as defined in NOAA IT Security Manual 212-1302, DOC IT Security Program Policy, and DOC IT Minimum Implementation Standards (2009). Since the operating system in ASOS, PSOS was not designed to provide more than a few basic security functions and it has not been supported by industry since 2005, the NWS was limited in its ability to comply with the DOC password policy. Another consideration was that NWS could not lock out users without impacting the availability of ASOS-generated weather data. Also, because FAA personnel in ATC towers and radar facilities did not have individual accounts on the FAA IT systems, the FAA would not allow individual passwords. In 2008, the NWS CIO waived the password policy to allow ASOS to continue to use group accounts and passwords. The waiver stipulated that the ASOS group passwords must comply with the DOC policy for group passwords and imposed an additional requirement that NWS change the group passwords every 60 days.

In 2008, the ASOS Configuration Control Board approved five requests for change (RC) submitted by NWS to modify the ASOS IT security capability, in part to comply with the terms of the password waiver. The ASOS Program Management Committee (APMC) agreed to fund the IT Security RCs. RC 10336 provided an improved password management capability. NWS awarded a task to its software contractor and the capability was developed in 2009 and tested (during Factory Acceptance Testing) in early 2010. NWS installed an interim version of the software (i.e., Build 3.03) on an ASOS at Sterling Field Support Center (SFSC). SFSC personnel used Build 3.03 to prepare and test this SOP.

1.1 System Overview

ASOS automatically observes, formats, archives and transmits surface weather observations. ASOS transmits an hourly report and a special report when conditions exceed pre-selected weather element thresholds (e.g., the visibility decreases to less than 3 miles). The telecommunications uses serial ports with no network connections. Any radio transmitting the observations to pilots on approach or for take-offs are confined to the airport and is a part of the FAA's suite of equipment and is outside the NWS' IT domain. ASOS uses various radio connections interacting with aircraft and between the sensors and the processing unit called the acquisition control unit (ACU). A number of ASOS units use underground cable instead of these radios to communicate data between the sensors and the ACU. ASOS reports the following basic weather elements:

- Sky condition: cloud height and amount (clear, few, scattered, broken, overcast, or total obscurations) up to 12,000 feet.
- Visibility (to at least 10 statute miles).
- Basic present weather information: type and intensity for rain, snow, and freezing rain.
- Obstructions to vision, e.g., fog, haze, and mist.
- Pressure: sea-level pressure, altimeter setting.
- Ambient temperature and dew point temperature.
- Wind: direction, speed, and character (gusts, squalls).
- Precipitation accumulation.
- Selected significant remarks including- variable cloud height, variable visibility, precipitation beginning/ending times, rapid pressure changes, pressure change tendency, wind shift, peak wind.

ASOS consists of an ACU, up to three data collection packages (DCP's), sensors that gather weather information, and user terminals. The ACU receives sensor data from the DCP(s); analyzes, compiles, and logs the data; and provides the data to the various ASOS users. The DCP controls the data collection process. It receives data from the individual sensors, formats the data, and transmits the data to the ACU. The DCP also provides and controls all primary electrical power to the sensors. The sensors gather the weather information. The sensor complement can consist of up to 16 sensors per remote DCP. These sensors perform specialized functions to gather raw data regarding weather and atmospheric conditions. These data typically include temperature, wind, and precipitation. The sensors are then either polled by the DCP or automatically transfer their data to the DCP where the data are incorporated into the ASOS data processing scheme. In addition to the sensors connected to the remote DCP, up to six sensors can be connected directly to the ACU. These sensors are referred to individually as local sensors, or collectively as the local DCP. The first three local sensor slots are reserved for pressure sensors contained inside the ACU.

ASOS automatically collects weather data and provides accurate, 24-hour accumulated weather reports to local weather observers; weather forecasters; airport personnel, including pilots and air traffic controllers (ATC's); and FAA and NWS personnel. ASOS functions include: measurement of weather elements, data processing and display, communication, and data storage (archiving). The ASOS is a flexible system with a modular construction that allows deployment in a variety of configurations for operation with or without the attendance of an observer. Unattended, the ASOS automatically collects, processes, and error checks data and formats, displays, archives, and reports the weather elements included in a surface weather observation. The ASOS also accepts inputs from observers (when present), who may override or add information to the automatically generated observation. Because of the flexibility of the ASOS, it can provide useful weather information in text and audio format to a variety of users.

1.2 ASOS User Interface

The Operator Interface Device (OID) provides the man-machine interface between users, either local or remote, and ASOS. A local ASOS user may sign on to the system as one of four specific user levels: Observer (OBS), Air Traffic Control specialist (ATC), Technician (TEC), or System Manager (SYS). A remote ASOS user must supply the remote access code within 1 minute after being prompted before access to the system is provided. The remote user then has two minutes to accept/reject the warning banner (yes/no). The remote user may then operate as an unsigned user or sign on to the system as either a TEC or SYS. If no interaction takes place between ASOS and the remote unsigned user for a period of 5-minutes, then the unsigned user will be automatically disconnected. The PRINT function is not available to the signed or unsigned remote users.

Each of the four user levels provides functionality associated with that level and may restrict access to system functions reserved for other user levels. ASOS users that do not sign on to the system are called unsigned users (UNS) and have access to ASOS observational data and SYSLOGs.

Following the power on sequence, the 1-Minute Screen will automatically appear on each configured OID. Displayed on this screen is a warning banner. The OID then displays each weather element, the last transmitted METAR or SPECI report, and the primary function keys. The individual weather elements are updated once each minute. If the user selected a screen other than the 1-Minute Screen and no interaction occurs within 2 minutes (except for TEC and SYS), the OID will automatically return to the 1-Minute Screen. After a user has been signed on for nine hours, or at the time of station closing, the user is automatically logged off, unless the user is an air traffic control specialist. The air traffic control specialist is exempt from this software feature. Command function (CMD) allows users signed onto the system to access ASOS system commands including generating corrected reports, voice message generation, assign and change system passwords, and use of the internal OID phone system.

1.3 ASOS Build 3.05

As described earlier, the ACCB approved five RCs listed in Table 1 and the APMC agreed to fund their implementation. RC 10336, as implemented in Build 3.05, provides an improved identification and authentication capability in ASOS.

Table 1. IT Security Requests for Change

RC Nr.	Title	Description
10336	Password	Group passwords to comply with DOC policy
10496	Warning Banner	Provide a warning banner for remote access and OID
10497	Audit Logs and Reports	Record more detailed information in AUDLOG
10577	Sensitive Station Settings	Protect elevation data with additional passwords
10651	Unsuccessful Logon Attempts	Create AUDLOG, make SYSLOG entries. Record unsuccessful logon attempts and expired passwords

The System Manager may change any password using the local or remote ASOS-ACU OID. In Build 3.05, ASOS checks for the following when the System Manager creates a group password and will accept a password only if it meets the following criteria:

- At least 12 characters. ASOS will support up to 20 characters.
- Six of the characters may only occur once in the password (e.g. ‘AAAAAAA123456’ is not acceptable, but ‘A%rmp2g3abcd’ and ‘A%ArmA2g3xyz’ are acceptable).
- It must contain characters from at least three of the following four categories:
    - English upper case characters (A...Z).

- English lower case characters (a...z)
- Base 10 digits (0...9) and
- Non-alphanumeric (For example, !,$#%).

Note, that for the first time ever, the ASOS user interface will accept both lower case and upper case characters. Build 3.05 provides feedback on the OID so that the user knows whether he/she is entering an upper case (U), lower case (L), numeric (N) or special character (S). All passwords including remote access code will expire in 60 days. Passwords are stored, in encrypted form, in BBRAM.

All group passwords and remote access codes will expire every 60 days per Department of Commerce policy in reference (e). The date of creation of the password will be stored in the password data structure. The password file is encrypted.

ASOS will generate a warning 14 calendar days before password expiry, on the OID and in the Audit Log (AUDLOG) and SYSLOG. The OID 1-MIN screen display is flashing yellow text when any user attempts to log in. The 60 day counter will start with the oldest date (of the remote access code and all of the group passwords) if the dates are not all the same. The password will still work after the expiration date. After the password expiration date, when any user logs on, a warning will be displayed on the OID 1-MIN screen (flashing yellow text) and both an AUDLOG and SYSLOG entry will be written. After successful logon the flashing yellow text will no longer be displayed during that session.

More than 5 repeated incorrect attempts to log on within 15 minutes will be treated as an intrusion attempt. ASOS will generate an entry in the AUDLOG and will generate a SYSLOG entry. ASOS will not lock a user out due to an unsuccessful log in attempt.

2 PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to describe the steps to follow in a cold start and during normal operations to change and manage passwords.

3 APPLICABILITY

Compliance with this SOP is required of all ASOS personnel.

4 PROCEDURES FOR BUILD 3.05 PASSWORD MANAGEMENT

4.1 Cold Start

Table 2. Procedures for a cold start.

Step	Account	Procedure
1	Technician	At OID, set power switch located on monitor base to ON position. The power-on indicator located in the left front of the CRT illuminates.
2	Technician	If ACU has a UPS, ensure that UPS POWER switch is set to off (0) position.
3	Technician	At ACU DC Power Supply Enclosure 1A5, ensure that ON/OFF switches on power supplies PS1 and PS2 are set to ON (1) position.
4	Technician	Set facility power circuit breaker for ACU to on position. If Class I ACU, power is applied to ACU cabinet components when facility power is applied.
5	Technician	If ACU has a UPS, set UPS POWER switch to on (1) position. Power is applied to components in Class II ACU cabinet.
6	Technician	With power applied to OID and ACU and after a brief warm up delay, OID displays the 1-minute display. If the display is not being updated, then on the numeric key pad, press the 0 (zero) key twice to refresh the screen. The data fields may contain the letter M, indicating that the sensor(s) are not reporting measurement data. If the message NEED SID AND AOMC PHONE message is displayed at the top of the screen, the system has lost its memory and requires a download of site specific data from the AOMC. In this case, perform the procedures in the S100.
7	Technician	TEC log in with default password. After the AOMC download then ASOS will log the TEC out[1] **Note: This is a new feature.**
8	Technician	Sign on the system as TEC with the password in the password file (case sensitive). Enter initials. The El-Tech must use his/her actual initials when logging on to ASOS**. Note: ASOS does not validate initials.**
9	Technician	Ensure that any other peripheral devices (VDU's, OID's, printer, etc) associated with the ACU are turned on.
10	Technician	Press REVUE-SITE-VERSN-AOMC to check status of all files. During the download, the VOICE/PASSW" data structure should change from "DOWNLOAD REQ" to "COMPLETED" and after some time it should change to "AUTO UPLOAD REQ".

4.2 Change a Password

[1] Only the TEC group is logged out of system after encrypted password file download.

Table 3. Procedures to change passwords.

Step	Account	Procedure
1	System Manager	Sign on as SYS. Select “CMD,” select “PASSW”
2	System Manager	Select the “PASSW” function key. A numbered menu with a prompt for user selection of the next action is displayed in the lower portion of the OID screen. Respond to the “SELECT ITEM TO BE CHANGED:” prompt with the menu number for the password to be changed. The display contains the following items: “SELECT ITEM TO BE CHANGED: 1. OBSERVER PASSWORD 2. TECHNICIAN PASSWORD 3. AIR TRAFFIC CONTROLLER 4. SYSTEM MANAGER PASSWORD 5. REMOTE ACCESS CODE 6. CRITICAL PASSWORD 7. EXIT” **NOTE: CRITICAL PASSWORD is a new feature.**
3	System Manager	A prompt to enter the old password for the selected user level will appears on the OID as follows: “ENTER OLD PASSWORD” Enter the current password for the selected user level. If the entered old password does not exactly match the system password for the selected user level, an audible tone sounds and an error message appears on the OID screen. If the entered old password matches the system password for the selected user level, an additional prompt to enter the new password for the selected user level appears as follows: “ENTER NEW PASSWORD” Enter the new password for the selected user level. A password may consist of 12 to 20 characters. The password must meet the specific requirements described in section 1.3 (i.e., be a strong password). Another prompt appears requesting that the new password be entered again to verify that there were no data entry errors: “ENTER NEW PASSWORD AGAIN” After the new password is entered again, if it does not match exactly the first entry of the new password, an audible tone sounds, an error message is displayed on the OID screen, and then the numbered menu is redisplayed. If the second new password entry matches exactly the first entry, then the numbered menu is redisplayed on the lower portion of the OID screen. If menu choice 5 (REMOTE ACCESS CODE) is selected, the procedure is the same as described above, except the word PASSWORD in all prompts is replaced by REMOTE ACCESS CODE. If menu choice 6 is selected for CRITICAL PASSWORD, then the user will use the SYS default password (the SYS default password used for cold

		starts) for the OLD CRITICAL PASSWORD. If menu choice 7 is selected, the numbered menu disappears from the OID screen and the user is returned to the 1-Minute Screen.

4.3 Remote Access to Change Station Elevation

Table 4. Procedures to change station elevation data.

Step	Account	Procedure
1	System Manager and Technician	Dial in to ASOS modem data link line.
2	System Manager and Technician	Warning Banner will appear. Select “Y”
3	System Manager and Technician	Enter the Remote Access Code.
4	System Manager and Technician	Sign on as SYS. Select “REVUE,” select “SITE,” select “PHYS,” select “CHANG.”
5	System Manager and Technician	Enter new value for station elevation.
6	System Manager and Technician	Respond with “Y” at the system prompt (Change Elevation from <old value> to <new value>? (Y/N))
7	System Manager and Technician	If user responded with ‘Y’, then user should be prompted for critical region password. Enter critical region PW.
8	System Manager and Technician	Verify that new station elevation is changed. Log out

4.4 NWSH prepare and distribute passwords table

The Office of Operational Systems (OOS) Observing Systems Branch will ensure that the password table is prepared and properly distributed to the FAA, NWS Regions, NCDC, AOMC, and OOS Maintenance Branch. Need to know will apply: The entire table will go to the AOMC, OPS12, and the NWS Regional focal points and the other organizations will receive only the passwords for the accounts they use (see Table 5). The password table will be encrypted prior to storage and transmission. The password table will be marked For Official Use Only (FOUO) and will be distributed only to authorized users with a need to know. The password table will include passwords and the remote access code.

Table 5. Distribution of passwords and the remote access code.

Organization	**SYS**	**TEC**	**OBS**	**ATC**	**CRIT**	**RAC**
FAA			X	X		
NOAA/NWS/NESDIS/NCDC						X
NOAA/NWS/OPS/AOMC	X	X	X	X	X	X
NOAA/NWS/OPS/FSOC/OPS22						X
NOAA/NWS/OPS/FSOC/OPS12	X	X	X	X	X	X
Data Users (user agreement with OPS12)						X
NWS Regions	X	X	X	X	X	X

4.5 NWS Regions coordinate transition from one password to another password

The Observing Systems Branch will advise the FAA, NWS Regional focal points, NCDC, AOMC, OPS22, and OPS12 within two to four weeks in advance of each password change. The Regional ASOS Manager can use EMRS to notify the Electronics Technicians (El-Tech) of the password change. The password table will have an alpha-numeric code associated with every password so that the new password can be referenced in EMRS. A central point of contact at the FAA will ensure that all FAA employees and contractors who need the new OBS and ATC passwords receive the passwords prior to NWS changing the passwords (remotely).

4.6 NWSH remotely access each NWS and FAA ASOS to change password

The Maintenance Branch, Office of Operational Systems will continue to set passwords and remote access code remotely at NWS and FAA ASOS sites using a software script and modem that dials into each ASOS, by region, and sets the passwords and remote access code. The Maintenance Branch also uses a software script to search SYSLOGs for selected codes on a regular basis. NOAA's NCDC provides the SYSLOGs each month.

4.6.1 Local System Manager change passwords

In addition to the Maintenance Branch, the System Manager can access an ASOS, either by local or remote OID, to change passwords.

5 STRONG PASSWORDS

ASOS checks for the items in Section 1.3 when the System Manager creates a group password:

The System Manager is responsible for the following (these requirements are not enforceable by the system). Passwords must not include any of following:

- Vendor/manufacturer default passwords
- Names (e.g., system user names, family names),
- Words found in dictionaries, addresses or birthdays,
- Common character sequences (e.g. 3456, ghijk, 24568).

6 ACCOUNT MANAGEMENT

6.1 NWS Regional Responsibilities for ASOS

Each NWS region coordinates ASOS operations and maintenance within the region, including IT security account management. Each NWS Region has a Division responsible for systems operations and maintenance and in most of the regions it is the System Operations Division (SOD). The Regional ASOS Manager, who in most of the regions is assigned to SOD, coordinates with the Office of Operational Systems at NWSH. The Electronics Program Manager (EPM) may delegate ASOS maintenance responsibilities to a Regional ASOS Manager. Either the EPM or Regional ASOS Manager coordinates with the ASOS maintenance personnel in the region. The Regional ASOS Manager has System Manager rights and permissions and is responsible for managing the ASOS accounts. The Regional ASOS Manager submits a list of ASOS System Managers for the region to the System Owner at NWSH; provides updates as personnel are assigned, reassigned, and terminated; and maintains a list of all NWS personnel authorized to access ASOS. As described in Section 4.4, the Regional ASOS Manager distributes ASOS passwords to the FAA facilities with ASOS.

6.2 System Manager Rights and Permissions

The SYS account group has the following IT security related rights and permissions:

- Access ASOS remotely with the remote OID mode and Direct Command Mode.
- Change passwords.
- Enter data in the system maintenance log.
- Ensure that passwords are changed every 60 days. Passwords are the remote access code and the passwords for the SYS, TEC, OBS, and ATC. In Build 3.05 an additional password, for sensitive station information will be included.

6.3 Electronics Technician at the NWS Forecast Office

The El-Tech follows authorized guidance (e.g., technical manuals, modification notes, maintenance notes) when maintaining ASOS. If the El-Tech can not access an ASOS he/she will contact the AOMC for assistance.

7 POINTS OF CONTACT

FSOC Focal Point for ASOS at Sterling Field Support Center

Primary: Ms. Jennifer Dover
NOAA's National Weather Service (OPS22)
Tel: 703-661-1259
Email: jennifer.dover@noaa.gov

Secondary: Mr. Juan Montenegro
NOAA's National Weather Service (OPS22)
Tel: 703-661-1206
Email: juan.montenegro@noaa.gov

ASOS Information System Security Officer

Mr. Jim McNitt
NOAA's National Weather Service (OPS22)
SSMC2, Room 4338
1325 East West Highway
Silver Spring, MD 20910
Tel: 301-713-2093 Ext 102
Fax: 301-713-2513
Email: james.mcnitt@noaa.gov

Comments and recommendations to this SOP are welcome. Forward any inputs to the ASOS Information System Security Officer by email: james.mcnitt@noaa.gov

8 REFERENCES

a. ASOS Software Users Manual
b. ASOS Site Technical Manual S100
c. ASOS Users Guide
d. Build 3.05 Factory Acceptance Test Procedures
e. Department of Commerce Interim Technical Requirements Nr. 009 (CITR-009), *Password Requirements*

APENDIX A ASOS Function / User Cross Reference

Table A-1. ASOS Function / User Cross Reference

Function	UNS	OBS	ATC	TEC	SYS	CRIT
SIGN Function	X	X	X	X	X	
Review Capability	X	X	X	X	X	
Print Capability (except remote users)	X	X		X	X	
Review METAR/SPECI Reports	X	X	X	X	X	
Review SHEF Messages	X	X		X	X	
Review 5-Minute Observations	X	X	X	X	X	
Review Daily Summary Products and Messages	X	X		X	X	
Review Monthly Summary Products and Messages	X	X		X	X	
Review 1-minute sensor data archived for the last 12 hrs	X	X		X	X	
Review 1-minute current sensor data	X	X		X	X	
Review Edit Log		X	X	X	X	
Review System Maintenance Log	X	X		X	X	
Review Communications Log	X	X		X	X	
Print the 1-Minute Screen with auxiliary data	X	X		X	X	
Activate and deactivate the audible alarms	X	X	X	X	X	
View auxiliary parameters	X	X	X	X	X	
Examine which sensors/parameters are in manual mode because of user editing of weather data	X	X	X	X	X	
Examine the release number and date of the installed operational software	X	X		X	X	
Access the system HELP function	X	X	X	X	X	
Generate SPECI reports using the current 1-minute observation		X	X			
Generate tornadic SPECI reports		X	X			
Transmit a SPECI Early/Transmit Corrected Reports		X				
Enter a tower visibility		X	X			
Cancel a pending SPECI report		X				
Edit and/or augment automatically generated weather products (1-minute observation)		X	X*			

Function	UNS	OBS	ATC	TEC	SYS	CRIT
Turn sensor report processing on or off.		X	X	X	X	
Add/change elements in daily and monthly summary products during the time periods the summaries are available for changing.		X				
Request 2-hour archive of 5-minute observations		X	X	X	X	
Select automated voice output for dial-in telephone and radio			X	X		
Manually record a 90-second message, i.e., NOTAM, at the end of the automated voice with the OID handset.			X	X		
Erase manually recorded 90-second voice message, i.e., NOTAM, just recorded.			X	X		
Playback manually recorded 90-second voice message, i.e., NOTAM, over the OID speaker.			X	X		
Change system configuration of sensors/display devices.				X	X	
Execute/review results of system diagnostic/tests.				X	X	
Change selected physical site constants.				X	X	
Change selected hardware configuration constants.				X	X	
Change station elevation (local OID)				X	X	
Change ceilometer elevation (local OID)				X	X	
Change station elevation (remote OID)				X	X	X
Change ceilometer elevation (remote OID)				X	X	X
Change selected external communications configuration constants.				X	X	
Change selected sensor configuration constants.				X	X	
Change selected ACU serial communications configuration.				X	X	
Make entries in the system maintenance log.				X	X	
Reset system hardware and software.				X	X	
Reset DCPs.				X	X	
Assign/change remote access code and passwords.					X	
Change selected site parameters: Special, local and SHEF alert criteria Site pressure data					X	
Process Hot Keys			X			

APENDIX B LIST OF ACRONYMS

ACU	Acquisition Control Unit
AOMC	ASOS Operations and Monitoring Center
APMC	ASOS Program Management Committee
ASOS	Automated Surface Observing System
ATC	Air Traffic Control
AUDLOG	Audit Log
CMD	Command Mode
DCP	Data Collection Package
EMRS	Engineering Management Reporting System
IS	Information System
IT	Information Technology
METAR	Meteorological Terminal Air Report and Meteorological Aviation Routine Weather Report
NCDC	National Climatic Data Center
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
OBS	Observer
OID	Operator Interface Device
QC	Quality Control
RC	Request for Change
SOD	System Operations Division
SOP	Standard Operating Procedure
SPECI	Aviation Selected Special Weather Reports
SYSLOG	System Log
SYS	System Manager
TEC	Technician
UNS	Unsigned
UPS	Uninterruptable Power Supply